PENDING CLAIMS AS AMENDED

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Please amend the claims as follows:

1.-34. (Canceled)

35. (Previously presented) A method for secure wireless communication using spread spectrum principles, comprising:

generating at least one pseudorandom number (PN) sequence;

generating at least one encryption sequence based on at least one of key and time-varying input;

combining the PN sequence with said encryption sequence to render an encrypted PN sequence; and

using the encrypted PN sequence to spread a communication signal.

36. (Previously presented) The method of Claim 35, wherein the communication signal is received from a data modulation component including a Walsh modulator.

37. (Previously presented) The method of Claim 35, wherein the encryption sequence is generated by a data encryption standard (DES) component or a triple-DES component.

38. (Previously presented) The method of Claim 37, wherein the DES component or the triple-DES component receives at least one multi-bit key and at least one time-varying input.

39. (Previously presented) The method of Claim 38, wherein the at least one multi-bit key is periodically refreshed.

40. (Previously presented) An apparatus for secure wireless communication using spread spectrum principles, comprising:

means for generating at least one pseudorandom number (PN) sequence;

means for generating at least one encryption sequence based on at least one of key and time-varying input;

means for combining the PN sequence with said encryption sequence to render an encrypted PN sequence; and

means for using the encrypted PN sequence to spread a communication signal.

41. (Previously presented) The apparatus of Claim 40, wherein the communication signal is received from a data modulation component including a Walsh modulator.

42. (Previously presented) The apparatus of Claim 40, wherein the encryption sequence generating means comprises a data encryption standard (DES) component or a triple-DES component.

43. (Previously presented) The apparatus of Claim 42, wherein the DES component or the triple-DES component receives at least one multi-bit key and at least one time-varying input.

44. (Previously presented) The apparatus of Claim 43, wherein the at least one multi-bit key is periodically refreshed.

45. (Currently amended) An apparatus for secure wireless communication using spread spectrum principles, comprising:

a pseudorandom number (PN) sequence generator configured to generate at least one PN sequence;

an encryption sequence generator configured to generate at least one encryption sequence based on at least one of key and time-varying input and further configured to combine the PN sequence with the encryption sequence to render an encrypted PN sequence; and

a spreader configured to use the encrypted PN sequence to spread a communication signal.

46. (Previously presented) The apparatus of Claim 45, wherein the communication signal is received from a data modulation component including a Walsh modulator.

47. (Previously presented) The apparatus of Claim 45, wherein the encryption sequence generator comprises a data encryption standard (DES) component or a triple-DES component.

48. (Previously presented) The apparatus of Claim 47, wherein the DES component or the triple-DES component receives at least one multi-bit key and at least one time-varying input.

49. (Previously presented) The apparatus of Claim 48, wherein the at least one multi-bit key is periodically refreshed.

50. (Previously presented) A processor for secure wireless communication using spread spectrum principles, said processor being configured to:

generate at least one pseudorandom number (PN) sequence;

generate at least one encryption sequence based on at least one of key and time-varying input;

combine the PN sequence with said encryption sequence to render an encrypted PN sequence; and

use the encrypted PN sequence to spread a communication signal.

51. (Previously presented) A computer-program product for secure wireless communication using spread spectrum principles, comprising:

a computer-readable medium comprising instructions for causing a computer to:

generate at least one encryption sequence based on at least one of key and time-varying input;

combine the PN sequence with said encryption sequence to render an encrypted PN sequence; and

use the encrypted PN sequence to spread a communication signal.

52. (Previously presented) A method for secure wireless communication using spread spectrum principles comprising:

generating at least one encryption sequence based on at least one of key and time-varying input;

combining a PN sequence with the encryption sequence to render an encrypted PN sequence; and

using the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

53. (Previously presented) The method of Claim 52 further comprising:

sending the despread signal to a Walsh demodulator.

54. (Previously presented) The method of Claim 52, wherein the encryption sequence is generated by a data encryption standard (DES) component or a triple-DES component.

55. (Previously presented) The method of Claim 54, wherein the DES component or triple-DES component receives at least one multi-bit key and at least one time-varying input.

56. (Previously presented) The method of Claim 55, wherein the multi-bit key is periodically refreshed.

57. (Previously presented) The method of Claim 55, wherein the time-varying input is at least one long code state.

58. (Previously presented) An apparatus for secure wireless communication using spread spectrum principles comprising:

an encryption sequence generator configured to generate at least one encryption sequence based on at least one of key and time-varying input;

a PN sequence generator configured to combine a PN sequence with the encryption sequence to render an encrypted PN sequence; and

a despreader configured to use the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

59. (Previously presented) The apparatus of Claim 58 further comprising:
a Walsh demodulator configured to receive a despread signal.

60. (Previously presented) The apparatus of Claim 58, wherein the encryption sequence generator comprises a data encryption standard (DES) component or a triple-DES component.

61. (Previously presented) The apparatus of Claim 60, wherein the DES component or triple-DES component receives at least one multi-bit key and at least one time-varying input.

62. (Previously presented) The apparatus of Claim 61, wherein the multi-bit key is periodically refreshed.

63. (Previously presented) The apparatus of Claim 61, wherein the time-varying input is at least one long code state.

64. (Previously presented) An apparatus for secure wireless communication using spread spectrum principles comprising:

means for generating at least one encryption sequence based on at least one of key and time-varying input;

means for combining a PN sequence with the encryption sequence to render an encrypted PN sequence; and

means for using the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

65. (Previously presented) The apparatus of Claim 64 further comprising:

means for sending the despread signal to a Walsh demodulator.

66. (Previously presented) The apparatus of Claim 64, wherein the generating means comprises a data encryption standard (DES) component or a triple-DES component.

67. (Previously presented) The apparatus of Claim 66, wherein the DES component or triple-DES component receives at least one multi-bit key and at least one time-varying input.

68. (Previously presented) The apparatus of Claim 67, wherein the multi-bit key is periodically refreshed.

69. (Previously presented) The apparatus of Claim 67, wherein the time-varying input is at least one long code state.

70. (Previously presented) A processor for secure wireless communication using spread spectrum principles, said processor being configured to:

generate at least one encryption sequence based on at least one of key and time-varying input;

combine a PN sequence with the encryption sequence to render an encrypted PN sequence; and

use the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

71. (Previously presented) A computer-program product for secure wireless communication using spread spectrum principles comprising:

a computer-readable medium comprising instructions for causing a computer to:

generate at least one encryption sequence based on at least one of key and time-varying input;

combine a PN sequence with the encryption sequence to render an encrypted PN sequence; and

use the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

Please add the following new claims:

72. (New) The method of claim 35, wherein the communication signal comprises a data symbol, and the method further comprises using the encrypting PN sequence to spread the data symbol.

73. (New) The apparatus of claim 40, wherein the communication signal comprises a data symbol, and the apparatus further comprises means for using the encrypting PN sequence to spread the data symbol.

74. (New) The apparatus of claim 45 wherein the communication signal comprises a data symbol, and the spreader further configured to use the encrypting PN sequence to spread the data symbol.

75. (New) The method of claim 52, wherein the received spread spectrum signal comprises a data symbol, and the method further comprises using the encrypting PN sequence to despread the data symbol to render a despread data symbol.

76. (New) The apparatus of claim 58, wherein the received spread spectrum signal comprises a data symbol, and the despreader further configured to use the encrypting PN sequence to despread the data symbol to render a despread data symbol.

77. (New) The apparatus of claim 64, wherein the received spread spectrum signal comprises a data symbol, and the apparatus further comprises means for using the encrypting PN sequence to despread the data symbol to render a despread data symbol.

78. (New) A base station for secure wireless communication using spread spectrum principles, comprising:

an antenna;

a pseudorandom number (PN) sequence generator configured to generate at least one PN sequence;

an encryption sequence generator configured to generate at least one encryption sequence based on at least one of key and time-varying input and further configured to combine the PN sequence with the encryption sequence to render an encrypted PN sequence; and

a spreader configured to use the encrypted PN sequence to spread a communication signal transmitted over the antenna.

79. (New) A user terminal for secure wireless communication using spread spectrum principles, comprising:

an antenna;

a pseudorandom number (PN) sequence generator configured to generate at least one PN sequence;

an encryption sequence generator configured to generate at least one encryption sequence based on at least one of key and time-varying input and further configured to combine the PN sequence with the encryption sequence to render an encrypted PN sequence; and

a spreader configured to use the encrypted PN sequence to spread a communication signal transmitted over the antenna.

80. (New) A base station for secure wireless communication using spread spectrum principles comprising:

an antenna;

an encryption sequence generator configured to generate at least one encryption sequence based on at least one of key and time-varying input;

a PN sequence generator configured to combine a PN sequence with the encryption sequence to render an encrypted PN sequence; and

a despreader configured to use the encrypted PN sequence to despread a spread spectrum signal received using the antenna to render a despread signal.

81. (New) A user terminal for secure wireless communication using spread spectrum principles comprising:

an antenna;

an encryption sequence generator configured to generate at least one encryption sequence based on at least one of key and time-varying input;

a PN sequence generator configured to combine a PN sequence with the encryption sequence to render an encrypted PN sequence; and

a despreader configured to use the encrypted PN sequence to despread a spread spectrum signal received using the antenna to render a despread signal.